LETTER FROM THE AUDITOR OF PUBLIC ACCOUNTS
KENTUCKY REVENUE CABINET

In Reference to the Statewide Single Audit
of the Commonwealth of Kentucky

For the Year Ended June 30, 2002

EDWARD B. HATCHETT, JR.
AUDITOR OF PUBLIC ACCOUNTS
www.kyauditor.net

144 CAPITOL ANNEX
FRANKFORT, KY 40601
TELEPHONE (502) 564-5841
FACSIMILE (502) 564-2912

CONTENTS

EDWARD B. HATCHETT, JR.
AUDITOR OF PUBLIC ACCOUNTS

To the People of Kentucky
Honorable Paul E. Patton, Governor
Dana Mayton, Secretary
Kentucky Revenue Cabinet

MANAGEMENT LETTER

This letter presents the results of our audit of the Kentucky Revenue Cabinet, performed as part of our annual Statewide Single Audit of the Commonwealth of Kentucky.

In planning and performing our audit of the financial statements of the Commonwealth for the year ended June 30, 2002, we considered the Kentucky Revenue Cabinet's internal control in order to determine our auditing procedures for the purpose of expressing an opinion on the financial statements and not to provide assurance on internal control. We noted certain matters involving internal control, compliance and its operation that we are including in this report. Some are considered to be reportable conditions under standards established by the American Institute of Certified Public Accountants.

Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of internal control that, in our judgment, could adversely affect the Kentucky Revenue Cabinet's ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statements.

A material weakness is a reportable condition in which the design or operation of one or more internal control components does not reduce to a relatively low level the risk that errors or irregularities in amounts that would be material in relation to the financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions.

Our consideration of the internal control would not necessarily disclose all matters in the internal control that might be reportable conditions and, accordingly, would not necessarily disclose all reportable conditions that are also considered to be material weaknesses as defined above.

Some findings are Other Matters that we have included in this report to communicate with management in accordance with Government Auditing Standards.

144 CAPITOL ANNEX
FRANKFORT, KY 40601-3448
502.564.5841
FACSIMILE 502.564.2912
ehatchett@kyauditor.net

105 SEA HERO ROAD, SUITE 2
FRANKFORT, KY 40601-5404
502.573.0050
FACSIMILE 502.573.0067

To the People of Kentucky
Honorable Paul E. Patton, Governor
Dana Mayton, Secretary
Kentucky Revenue Cabinet

Included in this letter are the following:

- Acronym List
- Findings (Reportable, Material and Other Matters)
- Summary Schedule of Prior Year Audit Findings

We have issued our Statewide Single Audit of the Commonwealth of Kentucky that contains the Kentucky Revenue Cabinet's findings, as well as those of other agencies of the Commonwealth. This report can be viewed on our website at www.kyauditor.net.

This letter is intended solely for the information and use of management and federal awarding agencies and pass-through entities and is not intended to be and should not be used by anyone other than these specified parties.

Respectfully submitted,

Edward B. Hatchett, Jr.
Auditor of Public Accounts

LIST OF ABBREVIATIONS/ACRONYMS

APA	Auditor of Public Accounts
BDC	Backup Domain Controllers
CIM	Compaq Insight Manager
Commonwealth	Commonwealth of Kentucky
FRC	File Requisition and Control System
FTP	File Transfer Protocol
FY	Fiscal Year
GOT	Governor's Office for Technology
HTTP	Hypertext Transfer Protocol
IIS	Internet Information Server
IIT	Individual Income Tax
KRC	Kentucky Revenue Cabinet
KRS	Kentucky Revised Statutes
LAN	Local Area Network
LSA	Local Security Authority
MFE	Modernized Front End
MSDE	Microsoft Data Engine
N/A	Not Applicable
NT	New Technology
PDC	Primary Domain Controller
RACF	Resource Access Control Facility
REV	Kentucky Revenue Cabinet
Revenue	Kentucky Revenue Cabinet
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
U.S.	United States

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 02-REV-1: The Kentucky Revenue Cabinet Should Ensure Confidential Taxpayer Information Is Protected And Preserved As Required By Statute

The Kentucky Revenue Cabinet (Revenue) collected 95% of the Commonwealth's total General Fund revenues, or $6,847,097,725 in tax receipts, and refunded $546,462,753 in overpayments to Kentucky taxpayers during the FY 02 audit period. We tested controls over Revenue's receipts, refunds, and accounts receivables and noted weaknesses at the central files repository that compromise Revenue's ability to comply with confidentiality and record retention laws.

We selected and tested samples of 58 corporate refunds, 42 corporate refund offsets, 42 individual income tax refunds, 42 receipts, and 72 receivables and noted the following problems during testing:

Revenue failed to provide tax returns totaling $6,604,779 in refunds to 18 corporate taxpayers; $6,516 in refunds to two (2) individual taxpayers; and, $722,551 in receipts and receivables from 13 Kentucky taxpayers. When tax returns are missing, we cannot determine if the returns were lost, stolen, destroyed, or ever received; thus, missing documentation causes us to question the legitimacy of a transaction, particularly when a refund is issued. Tax returns are the most persuasive evidence that is available to support that receipts and refunds are legitimate and properly recorded and classified within the financial statements. Since the primary objective of a financial audit is to obtain sufficient, competent, evidential matter to express an opinion over the financial statements, without original tax returns, we cannot verify the propriety of taxpayer receipts and refunds or provide reasonable assurance that financial statements are free of material misstatement.

- Revenue does not have the manpower and space required for maintaining five (5) years of tax returns for all Kentucky taxpayers, as required by KRS 131.185. Kentucky taxpayers filed 1,743,866 individual income tax returns for tax year 2000 alone, excluding tax returns filed by corporations and businesses. There are only 18 Revenue file room employees who are charged with the monumental task of maintaining order and ensuring accountability; thus, maintaining five (5) years of tax returns for every taxpayer in the Commonwealth is a tall order that has resulted in huge storage problems and backlogs in filing.

- Revenue does not enforce security procedures at the central files repository. We noted the file room doors were often left open and the entrance unattended. While security cameras are in place, they are not a substitute for keeping the doors closed, nor would they prevent someone from gaining unlawful access to confidential taxpayer information. Furthermore, Revenue breaches its own file room security policies by leaving the doors open and puts taxpayers at an unnecessary risk.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 02-REV-1: The Kentucky Revenue Cabinet Should Ensure Confidential Taxpayer Information Is Protected And Preserved As Required By Statute (Continued)

- Revenue does not effectively track requisitioned files. Tax returns that were requested for FY 98 audit testing were not returned to the central files repository to be refiled until the end of the FY 02 audit; four (4) years is an excessive amount of time for files to remain outstanding.

Revenue's FILENET system is not reliable. During FY 01, Revenue began scanning and imaging tax returns for access through FILENET, which was supposed to improve accessibility; however, according to various Revenue employees, FILENET is slow and inefficient. While FILENET has improved accessibility, it has not resolved the backlog at central files.

The backlog at central files is an ongoing problem that has been noted in prior year audits. Revenue has agreed with our recommendations, but the proposed solution of scanning and imaging through FILENET has not mitigated the problem.

A disorganized filing system compromises Revenue's ability to properly safeguard taxpayer information, as required by KRS 131.081 and 131.185. The benefits of retaining tax records are lost if the documentation cannot be easily located and retrieved at the central filing repository.

The APA annually audits the accounts of Revenue and the financial statements of the Commonwealth. Revenue is aware of the annual audit requirement and should also be aware of the necessity for maintaining tax documents in a manner that not only ensures compliance with confidentiality and record retention laws, but also ensures accountability to Kentucky taxpayers.

KRS 131.081 (15) states, "Taxpayers shall have the right to privacy with regard to the information provided on their Kentucky tax returns and reports, including any attached information or documents . . . no information pertaining to the returns, reports, or the affairs of a person's business shall be divulged by the cabinet to any person . . .."

KRS 131.185 states, "Income tax returns shall be kept for five (5) years; primary accounting records of tax payments, seven (7) years; and records containing all data of motor vehicle registration, three (3) years . . .."

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 02-REV-1: The Kentucky Revenue Cabinet Should Ensure Confidential Taxpayer Information Is Protected And Preserved As Required By Statute (Continued)

AU Section 801.05 states, "Management is responsible for ensuring that the entity complies with the laws and regulations applicable to its activities. That responsibility encompasses the identification of applicable laws and regulations and the establishment of controls designed to provide reasonable assurance that the entity complies with those laws and regulations. . .."

Revenue has a responsibility to uphold high standards of accountability.

Recommendation

Revenue should exhaust all resources to ensure that confidential taxpayer information is protected and preserved as required by statute and to ensure accountability to Kentucky taxpayers. Revenue should consider the following:

- Upgrading and expanding the use of the FILENET system or exploring the possibility of purchasing a more efficient system;
- Hiring temporary staff; or, if hiring additional staff is not possible,
- Enlisting the help of other Revenue employees to reduce the backlog at central files to ensure that taxpayer data is available and accessible.

Management's Response and Corrective Action Plan

Bullet Point 1: KRC has located all but four (4) of the documents originally requested.

Bullet Point 2: KRC does have the space required for maintaining all returns as required by the Records Retention Schedule. KRC does acknowledge the statement that additional manpower is needed at Central Files and will attempt to remedy this when budget constraints permit.

Bullet Point 3: KRC acknowledges the auditor's comments related to doors being left open at Central Files. The policy of maintaining security at Central files has been re-enforced with Revenue Operations Management and Central Files staff.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 02-REV-1: The Kentucky Revenue Cabinet Should Ensure Confidential Taxpayer Information Is Protected And Preserved As Required By Statute (Continued)

Management's Response and Corrective Action Plan (Continued)

Bullet Point 4: KRC's File Requisition and Control (FRC) system does have effective and efficient methods of tracking files. The files in question were requested by the Auditor of Public Accounts' office and never entered into the FRC system. The policy of having all requisitioned files entered into the FRC system has been re-enforced with Revenue Operations Management and Central Files staff.

Bullet Point 5: Performance failures in the FILENET system were primarily related to the failure of the mechanical jukebox used to store and retrieve the discs on which the images were stored. KRC has migrated to magnetic cache for storage purposes, thus eliminating the need for these juke boxes.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 02-REV-2: The Kentucky Revenue Cabinet Should Update The Sales Tax Database And Automate Processing Of Accelerated Tax Returns

We identified and tested 11 accelerated sales tax returns totaling $156,279,105. We noted the Revenue sales tax database does not process payments that equal or exceed $1,000,000; thus, a single transaction exceeding $1,000,000 will show up on the Revenue mainframe report as 999,999 in a succession of lines, with the bottom line total as the balancing amount. While this is a system limitation, data that is processed in this manner is difficult for end users to understand.

During FY 01, Revenue automated the processing of its high volume sales and use and withholding tax returns through the Modernized Front End (MFE) system. The MFE is used for scanning tax returns for posting to the Revenue mainframe, depositing receipts, and imaging returns for archiving purposes. Users across Revenue with access to the FileNet System are able to view images of all items in a transaction that are scanned into the MFE. Revenue is currently in the process of upgrading the MFE system to process accelerated tax returns; the changes should be implemented by July 2003.

While FY 01 financial statement information was not affected as a result of these weaknesses, the system limitations could affect the accuracy and reliability of the Revenue reporting system. Tax information that is not captured exactly as it is reported on the tax return makes it difficult to determine that receipts were recorded at the proper amounts and increases the likelihood that errors would go undetected by Revenue.

The system weaknesses, noted herein, represent deficiencies in the design of internal controls that could result in violations of laws and regulations that could materially affect Revenue's financial reporting. Good internal controls dictate that receipts should be properly posted to computer records from supporting documentation and all data processed by significant systems should be reviewed to determine accuracy and completeness.

Recommendation

We recommend Revenue take the following actions to correct these weaknesses:

- Update Revenue's mainframe system to process tax payments that equal or exceed $1,000,000; and,

- Complete the update of MFE to process all accelerated sales tax returns; this reduce manual processing and should increase mathematical accuracy, which would increase the reliability of the mainframe data. If this is not feasible, due to the magnitude of the tax payments involved, all accelerated sales tax returns should have a secondary level of review that includes verifying, editing and approving all adjustments.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 02-REV-2: The Kentucky Revenue Cabinet Should Update The Sales Tax Database And Automate Processing Of Accelerated Tax Returns (Continued)

Management's Response and Corrective Action Plan

KRC agrees that putting accelerated sales tax returns on the MFE will provide a more effective processing tool than the current environment. This recommendation is currently in process, but it will likely not occur until FY 04.

However, due to the current and projected budget deficit, it will be necessary for KRC to determine whether the cost of changing the sales and use tax mainframe system for this issue is a priority. While the data may be difficult for some users to understand, the total payment is represented in its entirety on the system. This change may be more easily achieved in the event the KRC builds a new sales and use tax system.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 02-REV-3: The Kentucky Revenue Cabinet Should Strengthen The Security Surrounding Administrator Accounts

During the vulnerability testing of Revenue machines, we found several instances of lax security over administrator accounts, resulting in the potential of machines being vulnerable to intrusion.

We examined 62 Revenue servers and found three (3) servers where the administrator account had not been renamed or disabled. Since these accounts cannot be locked out if the account is not renamed, these servers could be vulnerable to a brute force attack. Further, one (1) domain had 25 servers with administrator level accounts where passwords had not been changed from 131 to 841 days. These vulnerabilities existed as of June 30, 2002.

Further, we examined all Revenue controlled servers for specific applications running on port 1433 and found seven (7) that could be vulnerable. These seven (7) servers allowed the auditors to gain "Master" access through SQL using the default administrator logon. This type of access would provide an unauthorized user with complete access to the application. Further, the user would be granted local system account rights to the server on which the application resides.

Access to administrator accounts could provide unnecessary system privileges and can allow full access to the system. Therefore, these accounts should be secured as much as possible. At a minimum, the passwords for these accounts should be changed from the system defaults. Further, some administrator accounts could be renamed to help obscure them from an unauthorized user's view.

Recommendation

We recommend Revenue review all machines to ensure that the local administrator accounts have been changed from the default-naming conventions and have a password established. Further, all applications that might allow a user access to the system or to configuration settings should be reviewed to ensure that default logons are not allowed. Finally, Revenue should ensure all administrator accounts adhere to password policies by ensuring all passwords are changed at the established expiration interval.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 02-REV-3: The Kentucky Revenue Cabinet Should Strengthen The Security Surrounding Administrator Accounts (Continued)

Management's Response and Corrective Action Plan

KRC has reviewed all administrator accounts on all servers and have renamed the default administrator accounts. Using User Manager Pro software, we changed administrator account passwords on all servers and workstations in both the KRC and KRC_MFE domains. Strong passwords will be used on all administrator accounts. Procedures have been put in place for the KRC security staff to do this on a monthly schedule.

Seven (7) systems allowed the auditor to gain access to MSDE [Microsoft Data Engine] databases through using the default administrator logon of SA and a blank password. KRC previously checked and made sure that default administrator passwords on all our SQL servers had been changed. However, these systems all contained MSDE, which is like a run-time version of SQL, used for development and some applications. KRC has determined which applications require the administrator logon and have changed the account name and password. Most did not require the default logon account and it has been deleted.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 02-REV-4: The Kentucky Revenue Cabinet Should Ensure All Open Ports On Agency Machines Have A Business-Related Purpose

During the interim security vulnerability assessments for servers controlled by Revenue, we determined that there were several servers with ports open that may not have a specific business-related purpose. Additionally, we noted several web service vulnerabilities that indicate updated patches are needed. Due to the large number of issues, we have grouped the findings below by port number and application.

Port 7 – Echo and Port 19 - Chargen

We found two (2) servers that had both ports 7 and 19 open. These ports are not necessary for the function of the server, and could potentially be used to perpetuate a DoS attack.

Port 80 – HTTP

First, there were 11 machines with port 80 open that would not display the website. When no default page or restricted logon is required, normally this shows that there is no application/web service running at the port. Second, three (3) websites provided configuration information of printers or print servers. This situation allows too much access to an unauthorized or anonymous user. Third, one (1) website was the default page for Microsoft Windows NT 4.0 Option Pack. Revenue should review the necessity of this port. Finally, using one (1) assessment tool, we were able to determine that there may be several well-known web service directories present on two (2) servers that should be restricted from anonymous viewing. We were able to pull up several of these directories and see the pages without restriction.

Port 443 – HTTPS

Ten (10) servers were found with port 443 open but would not display a website. None of the ports appear to have an application/web service running on them.

Port 8000 – HTTP

One (1) server owned by Revenue was discovered that had port 8000 open. This website provided configuration information of a printer or print server. Once again, this situation allows too much access to an unauthorized or anonymous user.

Port 8080 – World Wide Web – Proxy

Two (2) machines were found with port 8080 open, which allowed access to the Oracle Servlet Engine web page. We were able to view the Error, Event, and HTTP logs for these servers. These pages should be restricted from anonymous viewing.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 02-REV-4: The Kentucky Revenue Cabinet Should Ensure All Open Ports On Agency Machines Have A Business-Related Purpose (Continued)

Other Ports

We discovered one (1) machine with Microsoft Personal Web Server 4.0 on it. An exploit of Internet Information Server (IIS) was used that allows access to the Disk Operating System (DOS) command line on the machine. We were able to search through folders on the C:\ and D:\ drives of the machine and found several interesting subfolders/files. Directory listings were allowed of the /cgi-bin/, /scripts/, and /_vti_bin/ folders. This permits an attacker to browse through scripts and executables within these directories, allowing them to target and exploit potential weaknesses.

There were three (3) machines in which the web service on Microsoft's IIS 4.0 has a buffer overrun vulnerability when a 3000+ character long request is made for an .htr file. This vulnerability could allow a remote attacker to execute arbitrary code and gain control of the computer.

We found the aexp2.htr on one (1) machine. From here, an attacker can launch password attacks against the local machine or proxy attacks against other machines on the network.

Two (2) servers had ports open that we were unable to specifically relate to known applications.

The existence of open ports is an invitation for intruders to enter the system. To minimize the risk of unauthorized access to a machine, only necessary, business-related ports should be open. Further, the application residing at these ports should be secured to the extent possible. Finally, proper maintenance requires that software patches be installed promptly on all servers to strengthen security.

Recommendation

We recommend Revenue perform a review of all open ports on the servers discussed in this finding. If there is not a specific, business-related purpose requiring a port to be open, then that port should be closed. Further, we recommend Revenue begin a periodic review of open ports on all machines owned by the agency to ensure necessity. Revenue should also ensure updated patches are installed on all servers under their control.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 02-REV-4: The Kentucky Revenue Cabinet Should Ensure All Open Ports On Agency Machines Have A Business-Related Purpose (Continued)

Management's Response and Corrective Action Plan

KRC reviewed all comments concerning questionable open ports found by the auditors office and have taken action to remove Web Services when not required. Also, KRC has applied all of the latest security patches from Microsoft and will, after evaluation, continue to apply patches as they become available. The review of open ports identified by the auditor's report prompted KRC to disable FTP and Web services on all servers unless it is absolutely necessary. KRC is developing a schedule of scanning all network servers for open ports and reviewing for any potential vulnerability.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 02-REV-5: The Kentucky Revenue Cabinet Should Ensure All User Accounts On The Agency Servers Are Necessary

During the interim vulnerability reviews of Revenue, we discovered several instances where accounts were established either on servers or for applications, but did not appear to be necessary.

First, we reviewed NetBIOS account information on 35 servers within three (3) of the Revenue domains, one (1) of which was the PDC for unused or disabled accounts. On the PDC within the KRC_MFE domain, there were 45 accounts that had not changed their password in more than 30 days, with 35 of them having never logged onto the system. There were also eight (8) accounts listed as disabled.

Second, we used three (3) different tools and attempted remote logon to known applications with default logon combinations. We were able to create a FTP session through port 21 on 12 machines with the anonymous or guest logins. Some of these servers allowed connection without having to provide any type of user ID or password.
Intruders often use inactive accounts to break into a network. If a user account has not been utilized for some time, the account should be disabled until it is needed. This minimizes the possibility that an unauthorized user will utilize the account. If an account is not going to be reinstated, then it should be deleted. Further, default administrator, guest, and anonymous accounts in operating systems and applications are some of the first accounts that an intruder will attempt to use. They should be assigned strong passwords or, where possible, renamed or removed immediately after installation.

Recommendation

We recommend that Revenue review accounts on all servers to determine which accounts have not changed their password within the last 31 days. These accounts should be evaluated to conclude if they are still valid accounts that are required for a business-related purpose. If not, the accounts should be disabled or deleted, depending on the necessity of reinstatement of the account. Further, Revenue should ensure that all machines with FTP services running on them restrict access to default, anonymous, or guest logons.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 02-REV-5: The Kentucky Revenue Cabinet Should Ensure All User Accounts On The Agency Servers Are Necessary (Continued)

Management's Response and Corrective Action Plan

Revenue has reviewed accounts on all servers and removed or renamed all default administrator accounts and guest login accounts. Using User Manager Pro software, we changed administrator account passwords on all servers and workstations in both the KRC and KRC_MFE domains. Strong passwords will be used on all administrator accounts. Procedures have been put in place for the KRC security staff to do this on a monthly schedule. The eight inactive accounts that were identified by the Auditors were reviewed and it was determined that they could be deleted. KRC reviewed the forty-five accounts on the KRC_MFE domain and have reduced the number to twenty-seven accounts. There are twelve more accounts that may be potentially be deleted within the next month. Only those accounts that are necessary as system accounts and to run services will be retained.

FINANCIAL STATEMENT FINDINGS

Material Weaknesses and/or Material Instances of Noncompliance

FINDING 02-REV-6: The Kentucky Revenue Cabinet Should Have A System In Place To Reconcile Critical Information

Revenue does not have a system in place to input or reconcile critical information to the mainframe system; this continues to be a problem for Revenue, as this has been reported during prior year audits. Thus, Revenue cannot be sure that reported amounts remitted are correct. While Revenue currently has a reconciliation project underway, there was no system in place at the time of our audit.

Revenue should have adequate systems in place to ensure all taxes due to Kentucky have been collected and all taxpayers are reporting key information in compliance with Commonwealth laws.

Recommendation

Revenue should develop a system for reconciling critical information.

Management's Response and Corrective Action Plan

KRC agrees with the audit findings. Programming is underway to create a system, which will identify exceptions in the amounts reported by taxpayers. It is expected that some data will be available to begin activity in late February 2003. However, modifications will in all probability be necessary to the system as the program evolves. Until this system is fully implemented, any attempt to perform the reconciliation will be primarily in a manual environment and extremely labor intensive. Some aspects of this system are now functional with assessment activity being performed.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 02-REV-7: The Kentucky Revenue Cabinet Should Implement A System For Crosschecking Motor Fuels Dealer Reports

Revenue's motor fuels tax section has a significant backlog in crosschecking motor fuels dealer reports. Fuel dealers and transporters file reports with the motor fuels tax section. The Transporter's Report of Motor Fuel Delivered (Form 72A098) is filed each month by transporters, which includes detail that lists every consignee to whom motor fuel was delivered, type of fuel, number of gallons, etc. The transporter must provide one duplicate of this report so that Revenue can associate it with the appropriate monthly dealer reports. The transporter reports are tracked to ensure that each licensee is filing a monthly report timely.

We tested 38 reports and noted 35 instances where motor fuels dealer reports were not crosschecked; Revenue was more than four (4) years behind on crosschecking at the end of FY 02 audit. While attempts are being made to reduce the backlog, Revenue is unable to hire additional staff, due to state budget constraints. This finding is a repeat of 01-REV-4 and has been a finding for several years.

When dealer reports are not crosschecked, there may be errors, omissions, and irregularities that are not detected timely.

Good internal controls dictate that all available resources are utilized for ensuring the accuracy of motor fuels reports.

Recommendation

Revenue should use existing resources to redesign the internal control structure in a manner that would ensure that the crosschecking of motor fuels dealer reports is completed at current staffing levels.

Management's Response and Corrective Action Plan

KRC agrees with the Auditor's findings. Loss of experienced personnel continues to impact this area. Additional resources have been hired and assigned to the backlog. During the month of January 2002 three new Revenue program officers completed their probation period in the Motor Fuels Tax Section. Backlog reduction is their number one assignment. Backlog reduction will remain a high priority assignment until it is achieved.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 02-REV-8: The Kentucky Revenue Cabinet Should Date Stamp Motor Fuels And Motor Vehicle Usage Tax Reports

Revenue oversees the collection of motor fuels and motor vehicle usage taxes. Motor fuels refunds are required to be filed within five (5) years of the initial gas purchase. Revenue date stamps motor vehicle usage tax recapitulation reports and motor fuels refund applications when received to document the receipt date of these time-sensitive reports.

We selected and tested samples of 25 motor vehicle usage tax recapitulation reports and motor fuels refund applications we noted 13 recap reports and two (2) refund applications that were not date stamped when received. Without a date stamp, there is no verifiable documentation of the receipt date to support the imposition of fines for late-filed reports or the timely filing of refund applications; as such, county clerks may be fined for not filing their recapitulation reports in a timely manner and motor fuels refunds may be issued in error.

Good internal control dictates that documents with mandated deadlines are date stamped to provide verifiable documentation of the receipt date.

Recommendation

Revenue should ensure that documents requiring documentation of receipt date are date stamped when received.

Management's Response and Corrective Action Plan

KRC acknowledges the Auditor's findings concerning two unstamped refund applications. Employees will be reminded of the importance of the procedure and supervisory staff will review the applications for compliance. In addition, envelopes from motor vehicle usage tax recapitulation reports are maintained for use in determining the receipt date of the report for refund purposes. Therefore, date stamps on these reports are not required.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 02-REV-9: The Kentucky Revenue Cabinet Should Distribute Receipts Prior To Year End

Revenue does not consistently handle local distribution journal vouchers. We compared accounts receivable to receipts and found, from FY 01 to FY 02, that apportioned vehicle property tax accounts receivable increased 19.3% ($311,187.54) and receipts increased 188.6% ($6,471,568.44). Also, the omitted tangible property tax – state accounts receivable increased 32.8% ($14,832,974.67) and receipts increased 51.1% ($1,837,698.08).

We discovered the huge increase in apportioned vehicle property tax receipts was the result of not making the local distribution until after the end of the fiscal year. For FY 01, Revenue made the distribution prior to June 30, prior to FY 00, it was done after the fiscal year-end. Revenue was advised by the Governors Office for Policy and Management to wait until after the year-end due to budget constraints.

The omitted tangible property tax receipts increase resulted from the 4th quarter local distribution not being made until after the year-end. Normally, the money is collected in the state account and transferred to the local distribution account prior to year-end. The distribution system then redistributes respective amounts to the local jurisdictions. However, for FY 02 the distribution was not made until the General Fund was swept after the fiscal year end.

By not processing the local distribution journal vouchers before the fiscal year-end, the General Fund receipts are overstated. The local distribution money does not belong to the state it is the property of the local governments and should not be included in the state's General Fund receipts at year-end.

GASB Codifications Statement 34, Section 1800.146 says, "Effective management control and accountability for governmental funds can best be achieved by using a common language and uniform classification system in financial planning, management, and reporting. The terminology and classifications discussed above provide such a common language. To the maximum extent practicable, the suggested terminology and classifications should be used consistently in all phases of budgeting, accounting, and reporting. [NCGAS 1, ¶126]."

Recommendation

Revenue should process local distribution journal vouchers before the fiscal year end in order to align receipts so that the fiscal year earnings are not overstated as of June 30th.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 02-REV-9: The Kentucky Revenue Cabinet Should Distribute Receipts Prior To Year End (Continued)

Management's Response and Corrective Action Plan

KRC management feels the method used to compute the distribution this past year is actually the better one since completed year-end data is available and estimates and adjusting entries do not need to be made to correct estimates made for the fourth quarter every year. There is no effect on the actual timing of the distribution to the local jurisdictions, merely a difference in when the journal voucher is done. By accounting for the distribution in the year-end financial closing package as estimated receipts to be refunded in the next fiscal year, the Cabinet accounts for the difference in timing between receipts and disbursements.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 02-REV-10: The Kentucky Revenue Cabinet Should Ensure That Individual Income Tax Refunds Are Properly Approved

Revenue's individual income tax (IIT) on-line refund system will not process refunds greater than $30,000; refund requests exceeding $30,000 are dropped out to the IIT Branch for manual processing and approval.

We tested a sample of 25 IIT refunds exceeding $30,000 and noted three (3) refunds, totaling $259,925, that were not properly authorized. Failure to properly authorize tax refunds could result in refunds that are issued in error or fraudulently.

Good internal controls dictate that tax refunds are properly authorized prior to issuance. Revenue's policies and procedures require the branch manager's approval for IIT refunds up to $100,000 and the division director's approval for refunds exceeding $100,000.

Recommendation

Revenue should follow procedures for ensuring proper approval of all refunds.

Management's Response and Corrective Action Plan

KRC disagrees with the finding that three refunds over $30,000 did not have proper authorization. The three returns in question had Refund Memo's attached which contained all required signatures by management staff. It appears the actual returns with the properly approved and validated Refund Memos were not reviewed during the audit.

Auditor's Reply

Auditor did not find evidence of signed refund memos in the individual income tax files examined when testing. The documents were presented by the agency after the audit finding was issued to Revenue. Proper procedures and filing should be consistently adhered to.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 02-REV-11: The Kentucky Revenue Cabinet Should Remove The Simple Network Management Protocol Service Or Change The Default Community String

During the interim vulnerability reviews of Revenue, the auditor found 12 servers that had the Simple Network Management Protocol (SNMP) service available and would allow an anonymous user to logon with the community name "public". The "public" community name is the default public account for this service. The use of the "public" community name allows too much information to be provided to any anonymous user. The auditor was given information about the system, such as listening ports, open sessions, active user accounts, and shares that exist.

Information provided by the SNMP service concerning a machine's functions could be useful to an intruder in developing an attack. Access to the world at large through default logons should not be allowed. To accomplish this, the agency should change the SNMP service default community names.

Recommendation

We recommend that Revenue either disconnect the SNMP service or change the "public" community name to a more sophisticated name on all servers. Further, any new machines should be checked for the SNMP service to ensure the "public" community name has been changed.

Management's Response and Corrective Action Plan

SNMP service had been loaded on some servers for the use of Compaq Insight Manager and as a default on some printers to provide web access. Since Compaq Insight Manager has not been deemed useful here at KRC and we do not allow web access to network printers, SNMP was removed from all printers and servers. This was completed on September 13, 2002.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 02-REV-12: The Kentucky Revenue Cabinet Should Ensure That Security Information Leakage Concerning Agency Devices Is Minimized

As was noted in the previous audit, Revenue did not restrict critical information divulged by their network servers. During the review of Revenue's local area network (LAN) security for FY 02, we discovered several instances where machines within the LAN provided information to anonymous users that could potentially help an intruder with developing details for an attack.

Using standard scanning tools we reviewed the names and other remarks for all servers located within three (3) of the Revenue's domains. We noted that the naming convention of servers was not sufficiently ambiguous to disguise the function of some of the servers. Further, there were remarks for three (3) machines that might catch an intruder's interest.

We also ran other vulnerability assessment tools twice during the fiscal year on 62 servers within the three (3) Revenue domains to determine if they would return information on Local Security Authority (LSA), Password Policies, or Valid User, Group, or Share Lists.

The following table depicts the number of servers that would provide this information:

Type of Information	Number of machines	Percentage of 62 machines providing information
LSA	50	80.6%
Password Policies	50	80.6%
Valid User List	50	80.6%
Valid Group List	47	75.8%
Valid Share List	47	75.8%

Finally, we found 20 servers with port 2301 open. We were allowed to logon to the Compaq Insight Manager (CIM) application on 16 of these servers with the default administrator user id and password. This access provides too much information to a potentially unauthorized individual.

For security purposes, detailed information concerning the specific servers or user accounts that contributed to these findings is being intentionally omitted from this comment. However, these issues were thoroughly documented and communicated to the appropriate agency personnel.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 02-REV-12: The Kentucky Revenue Cabinet Should Ensure That Security Information Leakage Concerning Agency Devices Is Minimized (Continued)

An agency's domain information that is accessible to the world at large through inquiry tools or default logons should be kept at a minimum. Agencies should ensure that information such as location, accounts associated with the server, data residing on the server, and the server's role is not divulged or is stated in the most minimal of terms. To accomplish this, an agency can set devices to not respond to certain types of inquiries, can use naming conventions that obscure the purpose of servers, can provide no comments on server activity, and can restrict access to default logons for applications.

Recommendation

We recommend that Revenue restrict the information that is being provided by its their LAN machines to anonymous users. First, the naming convention for servers should be altered to make them more ambiguous and any unnecessary comments associated with the servers should be removed. Second, boundaries should be placed on what types of responses servers provide based on certain inquiries. Third, the default logons for the CIM application should be changed.

Management's Response and Corrective Action Plan

KRC removed the remarks on all servers and, when possible, removed any other remarks from printers, desktops and laptops. KRC has started the renaming of servers with ambiguous names as servers are built or replaced. After some research, KRC found that the Netbios_fix.reg patch would prevent hackers from using the ENUM tool to obtain password policies and user, share and group lists from servers. This patch was applied to all KRC servers. This patch also keeps hackers from obtaining Netbios information on shares, groups and /or accounts. KRC discontinued the use of Compaq Insight Manager and decided to remove that software from all of their servers.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 02-REV-13: The Kentucky Revenue Cabinet Password Policy Should Be Consistently Applied To All Local Area Network Servers

As was noted in the prior audit, password policies established on certain critical Revenue servers did not adhere to the agency password policies. During the FY 02 audit, we reviewed the password policies of all Primary Domain Controllers (PDC), Backup Domain Controllers (BDC), Structured Query Language (SQL), and a sample of Network (NT) servers within the three (3) main domains maintained by Revenue, for a total of 62 servers. We were able to obtain the password policies for 58 of these servers out of 62 reviewed.

It was found that the password policies established on 11 NT servers within two (2) Revenue domains did not agree to the agency password policy set forth in their Standard Procedure #5.2 – User id and Passwords. See the table below for findings:

Security Measure	Standard	Number of machines not in compliance with policy	Percentage of 58 machines not in compliance with policy
Maximum Age	30 days – GOT	11 – 42 days	19%
Minimum Age	0 day – GOT	11 – None	19%
Minimum Length	8 characters – GOT	11 – None	19%
Lockout Threshold	3 attempts – GOT	11 – None	19%
Lockout Duration	"Forever" – Industry Standard FASNTSB is set for 71,582,788 minutes (approximately 136.2 years)	11 – 30 minutes	19%
Lockout Reset	999 minutes – GOT	11 – 30 minutes	19%

Improvements were made after the FY 01 audit in which Revenue did change the password policy for PDC, BDC, and SQL servers not in agreement with the agency-set policy. However, NT servers should have been reviewed to ensure they were in compliance as well.

To help ensure the security of a network, it is necessary for a strong password policy to be developed and implemented on all servers within the network. If servers within a network are not sufficiently secured, the network could be compromised through one of these more vulnerable paths.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 02-REV-13: The Kentucky Revenue Cabinet Password Policy Should Be Consistently Applied To All Local Area Network Servers (Continued)

Recommendation

We recommend that Revenue review all servers within their agency-owned domains to ensure that the password policy established on all servers complies with the guidelines specified by the agency.

Management's Response and Corrective Action Plan

KRC has reviewed the password policy on all servers and has made the appropriate changes so that all servers in the KRC domains comply with the KRC Standard Procedure 5.2-Userid and Passwords. KRC will take action to ensure that this strong password policy is followed when building and administering all network servers.

SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
FOR THE YEAR ENDED JUNE 30, 2002

Fiscal Year	Finding Number	Finding	CFDA Number	Questioned Costs	Comments
Reportable Conditions					
(1) Audit findings that have been fully corrected:					
There were no findings for this section.					
(2) Audit findings not corrected or partially corrected:					
FY 01	01-REV-1	The Revenue Cabinet Should Update The Sales Tax Database And Automate Processing Of Accelerated Tax Returns	N/A	0	Revenue is working on automating accelerated tax returns, but it will likely not occur until FY 04. See 02-REV-2
FY 01	01-REV-3	The Revenue Cabinet Should Have A System In Place To Reconcile Critical Information	N/A	0	Revenue has a reconciliation project underway that is expected to begin in February 2003. See 02-REV-6
(3) Corrective action taken is significantly different from corrective action previously reported:					
There were no findings for this section.					
(4) Audit finding is no longer valid:					
There were no findings for this section.					

SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
FOR THE YEAR ENDED JUNE 30, 2002

Fiscal Year	Finding Number	Finding	CFDA Number	Questioned Costs	Comments
Material Weaknesses					
(1) Audit findings that have been fully corrected:					
FY 01	01-REV-3	The Revenue Cabinet Should Substantially Improve All System Related Controls Surrounding The Modernized Front End System	N/A	0	Resolved during FY 02.
(2) Audit findings not corrected or partially corrected:					
There were no findings for this section.					
(3) Corrective action taken is significantly different from corrective action previously reported:					
There were no findings for this section.					
(4) Audit finding is no longer valid:					
There were no findings for this section.					
Other Matters					
(1) Audit findings that have been fully corrected:					
FY 00	00-REV-1	The Revenue Cabinet Should Review Data Entry Logs To Ensure Completeness And Appropriateness Of Data Entry Procedures	N/A	0	Resolved during FY 02.
FY 01	01-REV-6	The Revenue Cabinet Should Review Data Entry Logs To Ensure Completeness And Appropriateness Of Data Entry Procedures	N/A	0	Resolved during FY 02.
FY 01	01-REV-7	The Revenue Cabinet Should Improve Security Controls for TSO Logical Access	N/A	0	Resolved during FY 02.

SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
FOR THE YEAR ENDED JUNE 30, 2002

Fiscal Year	Finding Number	Finding	CFDA Number	Questioned Costs	Comments
Other Matters					
(1) Audit findings that have been fully corrected (Continued):					
FY 01	01-REV-8	Revenue Should Establish A Formal System To Manage Processing Errors	N/A	0	Resolved during FY 02.
***(2) Audit findings not corrected or partially corrected*:**					
FY 97	KRC–7	The Revenue Cabinet Should Properly Safeguard Corporation Tax Returns	N/A	0	Exceptions were noted during FY 02 testing.
FY 98	KRC-1	The Revenue Cabinet Should Properly Safeguard Returns	N/A	0	Exceptions were noted during FY 02 testing.
FY 98	KRC-3	The Revenue Cabinet Should Ensure That Motor Fuel Reports Are Cross-Checked as Required	N/A	0	Exceptions were noted during FY 02 testing.
FY 01	01-REV-4	The Revenue Cabinet Should Implement A System For Crosschecking Motor Fuels Dealer Reports	N/A	0	Revenue has hired three new personnel to work only on the backlog. They will continue to work in this area until the backlog is resolved.

SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
FOR THE YEAR ENDED JUNE 30, 2002

Fiscal Year	Finding Number	Finding	CFDA Number	Questioned Costs	Comments
Other Matters					
***(2) Audit findings not corrected or partially corrected (Continued)*:**					
FY 01	01-REV-5	The Revenue Cabinet Should Ensure That All Tax Files Are Safeguarded	N/A	0	During FY 02, numerous problems were noted at Central Files; these problems were not solved by use of the FILENET system. This finding has been upgraded to a reportable condition for FY 02.
FY 01	01-REV-9	Revenue Password Policy Should Be Consistently Applied To All Local Area Network Servers	N/A	0	Exceptions were noted during testing for FY 02.
FY 01	01-REV-10	Revenue Cabinet Should Ensure That Information Leakage Concerning Agency Devices Is Minimized	N/A	0	Exceptions were noted during testing for FY 02.
(3) Corrective action taken is significantly different from corrective action previously reported:					
There were no findings for this section.					
(4) Audit finding is no longer valid:					
There were no findings for this section.					